

**16 FEBRUARY 2004**



**Operations**

**AIR FORCE ANITITERRORISM (AT)  
STANDARDS**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>

---

OPR: 3 AF/A38 (SStg Chirstopher Dunning)

Certified by: 3 AF/CC  
(Major General Michael W. Wooley)

Pages: 7

Distribution: F

---

This instruction implement Air Force Policy Directive 10-2, Readiness. It applies to all 3d Air Force (3 AF) Installations. Commander, United States Air Forces in Europe (COMUSAFE) Antiterrorism Plan (AT) Plan 10-245 provides vast AT guidance and to prevent duplication, this 3 AF instruction will provide specific AT guidance for items that must be routed through HQ 3AF for review, coordination, or approval.

**1. Assignment of Force Protection (FP) Responsibility:**

1.1. Tactical control (TACON) for FP is inherent in combatant command authority. The combatant commander delegates TACON for FP responsibility to component service commanders through country specific MOA. The matrices attached to the MOAs outline service responsibility for FP for all noncombatant commander elements in the country. Force protection does not skip echelons. COMUSAFE broadly delegates FP responsibility to numbered air force (NAF) commanders. NAF commanders assign specific responsibilities for force protection of Department of Defense (DoD) personnel and assets to installation commanders to assess and mitigate risk to missions assigned to USAFE.

1.2. TACON for FP enables commanders to order implementation of force protection measures and to exercise authority over all security programs governed by DoD/Department of State Universal Memorandum of Understanding, Agreement (MOU/MOA) and respective Combatant Commander-Chief of Mission (COM) MOAs. It also authorizes commanders to change, modify, prescribe and enforce force protection measures for all DoD elements and personnel under the combatant commander for force protection. TACON for force protection includes the authority to inspect, assess security requirements, to direct DoD activities to identify the resources required to correct deficiencies, and submit budget requests to parent organizations to fund identified corrections.

1.3. Installation commanders are required to take appropriate action to execute AT/FP programs for all personnel and activities under their command. This includes all organizations, geographically sep-

arated units, tenant organizations and noncombatant commander assigned elements regardless of service. Local host-tenant agreements should be executed to specify command relationships as well as AT/FP support and funding arrangements for each tenant unit.

FP responsibility for geographically separated units is based on proximity to the unit in the best position to provide support, oversight, and command and control.

1.4. The 3 AF/CC maintains TACON for FP responsibility for all installations identified in the USAFE FP responsibility matrix. Third Air Force Chief Security Forces (Third Air Force/A38) will validate the USAFE FP responsibility matrix through the installation Antiterrorism Officers (ATO). The installation ATOs must ensure that the installation commanders review the matrix. Installation ATOs have until **7 February** of each year to complete the review. 3 AF/A38 will route for approval of the 3 AF/CC and forward to USAFE/SFP, no later than **15 February** of each year. All units must thoroughly review the subordinate units' matrices to ensure compliance.

1.5. Once installation commanders become aware of the force protection issues for an installation or activity, and have visited the facilities, they then become directly accountable for the force protection status of the installation, activity.

1.5.1. Commanders must be proactive in all matters pertaining to force protection. Commanders must study the force protection assessments and then visit the installations, activities under their command. They must work diligently to fix what they can, and elevate those items that cannot be resolved at their level. Force protection enhancement efforts should be approached in the following manner:

1.5.1.1. Installation commanders must elevate force protection issues through their chain of command until resolved. Installation commanders will elevate issues that are blocked due to diplomatic impasses (host nation support) to the 3 AF/CC. If not resolved, the 3 AF/CC will notify COMUSAFE. Again if not resolved, COMUSAFE will notify the Commander, United States European Command (USEUCOM), who in turn will notify "in writing" the ambassador and Secretary of Defense (SECDEF).

1.5.1.2. When there are apparent resource limitations, ensure that costs and financial requirements are measured on a cost-benefit basis. Commanders must prioritize these requirements in their unit programming and budgetary process. When unable to obtain the necessary resources locally, elevate the total (prioritized) bill up the chain of command while simultaneously working interim measures to fix the problem.

## **2. Antiterrorism Officer Appointment:**

2.1. Installation commanders will designate, in writing, a commissioned officer, noncommissioned officer (E-6 or higher) or civilian staff officer as ATOs for each installation, base or deploying organization. Primary and alternates must be assigned. ATOs will be trained in accordance with COMUSAFE AT Plan 10-245, Standard 6.

2.1.1. The appointed ATOs will validate this appointment letter annually and forward to 3 AF/A38 and to HQ USAFE/SFP, NLT **7 February** each year. HQ USAFE/SF or 3 AF/A38 may request an out-of-cycle update at any time.

2.1.2. Other AT staff personnel (program managers) do not have minimum rank requirements.

- 2.2. The Commander (3 AF/CC) will appoint 3 AF/A38 personnel as the Numbered Air Force (NAF) ATO and program manager.
- 2.3. All deploying units must appoint a trained ATO for each deployment. Appointed ATOs must contact 3 AF/A38 at least 6 weeks prior to the departure date (if possible).
- 2.4. Each tenant unit and noncombatant commander assigned elements not located on the installation will appoint an ATO and identify them to their respective host installation with TACON FP responsibility.

### 3. Vulnerability Assessment Management Program 6 (VAMP 6):

- 3.1. All personnel requiring access to the VAMP 6 must be appointed by the installation commander. The Directorate Security Force (USAFE/SF) maintains the right to determine whether or not someone will have access to the VAMP.
  - 3.1.1. There are different access levels for users of the VAMP and each level must be identified (ATO, installation VAMP administrator, Wing/CC, NAF ATO) on the appointment letter. The installation VAMP administrator may perform review functions of the installation commander but must be appointed in writing.
  - 3.1.2. ATOs must maintain a list of personnel requiring access to the VAMP. This list must be validated semi-annually and forwarded to 3 AF/A38 by **1 April and 1 October**. The 3 AF/A38 will provide the reporting format.
- 3.2. The 3 AF/A38 will consolidate the 3 AF main operating bases (MOB) lists and forward to HQ USAFE/SFP for action. All units may submit for new VAMP accounts or deletion of accounts at any time.
- 3.3. Installation ATOs will validate all information in the VAMP for their installation and edit and, or, update prior to the **last duty day of each month**.
- 3.4. Installations must enter into the VAMP, known critical vulnerabilities identified during a higher headquarters assessment **no later than 10 duty days after the outbrief**. Installations must input all other vulnerabilities identified by HHQ assessment **no later than 30 days upon receipt of the written report**.
- 3.5. The 3 AF/CC review will be conducted only after each installation commander has conducted a final review. The VAMP will send 3 AF/A38 with a notification message upon completion of installation commander review. The 3 AF/A38 will review and coordinate for 3 AF/CC review NLT 30 days of notification message.

### 4. Combating Terrorism Readiness Initiatives Fund (CbTRIF):

- 4.1. All CbTRIF submissions should go directly to Headquarters USAFE Force Protection Division (HQ USAFE/SFP), with a courtesy copy provided to 3 AF/A38.
- 4.2. CbTRIF packages for emergent needs must be submitted to USAFE/SFP prior to **1 September and 1 January** for the EUCOM 1 October and 1 February deadlines respectively. CbTRIF packages for emergency needs can be submitted anytime. An example of an emergency need would be a perimeter fence washed away by flooding.

4.3. All submissions will be IAW format in COMUSAFE AT Plan 10-245 and will be transmitted via Secure Internet Protocol Router Network (SIPRNET) only.

## 5. Level I Antiterrorism Awareness Training Statistics and AT Plan Status

5.1. According to COMUSAFE AT Plan 10-245, "Commanders will report the status of their AT Program and Training statistics every quarter."

5.2. Level I AT Awareness reports will be submitted to 3 AF/A38 NLT **3 January, April, July, and October**.

3 AF/A38 will consolidate all 3 AF installations reports and forward to HQ USAFE/SFP by 5 January, April, July and October of each year.

5.3. AT plans must establish and identify the responsible position, person in each unit for tracking Level I AT training.

5.4. Installations will report the status of their AT Plan as part of the quarterly Level I AT Awareness report. Sample format is provided in Tab A to Appendix 8 to Annex M to COMUSAFE AT Plan 10-245.

## 6. AT/FP Design Standards

6.1. Installation commanders will submit to HQ USAFE/CE their plan to evaluate existing inhabited structures (including family housing containing 13 or more units) in accordance with paragraph 3b of USEUCOM AT/FP OPORD 01-01. HQ USAFE/CE will coordinate plans through the USAFE staff for review and when approved by COMUSAFE, forward the coordinated package to HQ USEUCOM. These reports will be due annually on **15 February**. ATOs will submit a courtesy copy to 3 AF/A38 for NAF review.

6.2. Waiver process: The HQ USEUCOM Chief of Staff is the approval authority for any deviation (exception, waiver or variance) to the AT/FP construction design standards contained in USEUCOM AT/FP OPORD 01-01. Commanders must use all means necessary to meet these standards and shall strive to eliminate all waivers within their areas of responsibility. Waivers will be considered if compliance with the standard at a particular installation or facility will adversely affect mission accomplishment, unacceptably affect relations with the host nation, exceed local capabilities, or require substantial expenditure of funds at a location where forces will be removed or relocated in the near future. If a waiver request is unavoidable, all packages must be submitted through the 3 AF/CC to HQ USAFE/SFP. USAFE/SFP will coordinate the package through the USAFE staff for review and if approved by COMUSAFE, forward the coordinated waiver request package to HQ USEUCOM. Refer to D-1-A-1 of USEUCOM OPORD 01-01 for sample waiver format.

6.2.1. A request for a waiver will be submitted to 3 AF/A38 for the NAF review. If the 3 AF/CC approves, the waiver will be forwarded to USAFE/SF for review. Although the HQ USEUCOM Chief of Staff is the approval authority, the 3 AF/CC may disapprove a waiver request if deemed necessary.

## 7. Frequency Requests:

7.1. Deploying units will submit their frequency proposals in the standard frequency action format through Third Air Force Chief, Comm and Information Division (3 AF/A6) with an information copy to USAFE CSS/SCOF.

7.2. All units within the 3 AF AOR will submit their proposals through 3 AF/A6 for action/coordination.

## **8. Local Vulnerability Assessments (LVA):**

8.1. Installations commanders are required to conduct an LVA annually. These local assessments must include all activities and elements residing as tenants on installations, or geographically separated but under the TACON of the local commander for AT/FP, as defined in the Combatant Commander-COM MOA and accompanying matrix.

8.2. All identified vulnerabilities from an LVA must be submitted to 3 AF (POC: 3 AF/A38) for review by the 3 AF/CC.

## **9. Force Protection Compliance**

9.1. Commanders must report the status of the FP compliance for the host installation, GSUs, and noncombatant commander assigned elements. This report will be due to 3 AF (POC: 3 AF/A38) **NLT 1 April and 1 October** each year. The status of FP compliance must include:

- 9.1.1. Dates of last local vulnerability assessment (VA)
- 9.1.2. Dates of next local vulnerability assessment (or HHQ VA)
- 9.1.3. Date of AT/FP Plan
- 9.1.4. Date of last Program Review
- 9.1.5. Whether or not compliant with current FPCON measures
- 9.1.6. Date of local threat assessment for each installation, location

9.2. Installation commanders, in coordination with the installation Threat Working Group (TWG) and/or Force Protection Working Group (FPWG), shall review local FPCON measures semi-annually to ensure threat mitigation measures are appropriate.

9.2.1. Installation commanders must forward any request, waiver to deviate from HHQ directed RAMs and FPCONs to the 3 AF/CC. 3 AF/A38 will act as the intermediary with the installation ATO. If a higher authority is required to approve deviation, 3 AF will route accordingly.

9.2.2. All tenant units and noncombatant commander assigned elements must submit waiver requests through the MOBs, approved by the MOB installation commander.

9.3. ATOs will forward all TWG minutes and Battle Staff Directives to 3 AF/A38 to ensure compliance with HHQ directives and to keep the 3 AF/CC aware of the FP status.

## **10. NAF ATO Responsibilities**

10.1. The 3 AF/A38 will develop procedures to ensure each deployment in their AOR has an assigned ATO and AT plan.

10.2. The 3 AF/A38 will coordinate with deploying units to ensure an ATO is assigned and an AT plan is developed. This will only apply to deploying units, expeditionary units and not for each deploying UTC (e.g., if 999 AW deploys the 99 EAW to a location that does not have an established AT program or plan, an AT plan must be written prior to the deployment).

10.3. All deployment AT plans must be sent to 3 AF/A38 at least 30 days prior to the departure date. These plans must be coordinated and approved by the deploying commander. The appointed ATO for the deployment may contact 3 AF/A38 to determine if a plan has been accomplished for a particular location by a previous deploying unit.

MICHAEL W.WOOLEY, Major General, USAF  
Commander

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

COMUSEUCOM AT/FP OPORD 01-01 FRAGO 1, 8 March 02

AFI 10-245, *AF Antiterrorism Standards*

DoD Directive 2000-12, *DoD Combating Terrorism Program*

DoD Handbook 2000.12-H, *Protection of DoD Personnel Against Terrorist Acts*

DoD Instruction 2000.16, *DoD Combating Terrorism Program Standards*

***Abbreviations and Acronyms***

**AOR**—area of responsibility

**AT**—antiterrorism

**ATO**—antiterrorism officer(s)

**CbTRIF**—combating terrorism readiness initiatives fund

**COM**—Chief of Mission

**COMUSAFE**—Commander, United States Air Forces in Europe

**DoD**—Department of Defense

**FP**—force protection

**FPCON**—force protection condition

**LVA**—local vulnerability assessment

**MOA**—Memorandum of Agreement

**MOB**—main operating base

**MOU**—Memorandum of Understanding

**NAF**—numbered air force

**NLT**—not later than

**RAM**—random antiterrorism measures

**SECDEF**—Secretary of Defense

**SIPRNET**—Secure Internet Protocol Routing Network

**TACON**—tactical control

**USEUCOM**—United States European Command

**UTC**—unit type code

**VAMP**—Vulnerability Assessment Management Program